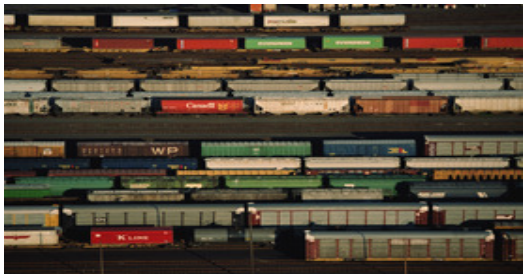

The Role of Governments in Improving Freight Logistics in Queensland

Working Paper 3: Transport Security

Clara Tetther and Luis Ferreira

December 2004

Queensland Government
Queensland Transport

QUT

Queensland Government
Department of Main Roads

EXECUTIVE SUMMARY

This report represents the third deliverable of a research project funded jointly by Main Roads and Queensland Transport aimed at identifying the role which all levels of government can play in the process of implementing change in the freight logistics (FL) sector in Queensland.

General

- Security is becoming a necessary and essential cost of doing business.
- Transportation is a potential and attractive target, that also plays a vital role in:
    - Prevention and detention
    - Monitoring and mitigation
    - Response and recovery.
- Growing reliance on virtual systems for control and monitoring opens up vulnerabilities in the communications and virtual transport networks.
- Threats to transport security can be in the form of:
    - Direct physical attack (bombing of infrastructure, hijacking, etc.)
    - Direct operation attack (viral attack on critical systems, tampering with communication channels, etc)
    - Tampering with legitimate cargo (introducing biotoxins, etc.)
    - Use of vehicles as weapons of destruction (9/11 attacks).
- Certain elements of the transport infrastructure (eg: the Sydney Harbour Bridge, and other landmarks, are cultural and Western symbolic icons, adding further appeal to terrorism targets.

Supply chain security - the hidden costs

- Any security attack can have reaching implications beyond ‘damage’ costs.
- Costs of implementing transport security may involve delays and productivity losses.
- Who will bear the costs ‘user’, ‘polluter’, or ‘beneficiary’?
- Security is seen as ‘public good’ - hence not an attractive ‘investment’ in the competitive market.
- Potential cost and magnitude of security task in the transportation sector means that it must be approached systematically and effectively.
- Intelligent decision making and assessment tools may potentially assist in the efficient allocation of security resources in targeting high-risk assets and activities.

Securing the supply chain: the problems

- Transport network is extensively diverse, necessarily accessible, ubiquitous and entwined in the economy and the community.
- Fully integrating security will take many decades, as new systems are developed and implemented, assets are gradually modified and replaced, standard guidelines and regulations are proposed and implemented.
- Diversity of users, owners and operators and the extent of the network create a system in which it is almost impossible to totally protect each potential target or perceived vulnerability.
- A potentially workable solution includes a layered and holistic approach.

The integrity of the supply chain: common threats

- Crime, especially in road transport is currently unreported, thereby increasing the difficultly in accurately assessing the vulnerabilities.
- Due to the extent of vulnerabilities and the potential cost of security, security efforts need to be dual-use, efficient and adaptable.
- Need to prioritise security criticality so that resources can be assigned effectively.
- Need to mesh security measures with other objectives, such as curbing theft, tracking and monitoring cargo, asset management and assuring safe operations.
- Intelligence-driven analysis used to detect threats in the virtual network may be adaptable to use in the physical transport network. These methods can enhance the traditional risk assessment for better control and justification of budget and resource decisions.

Security needs assessment

- Infrastructure needs to be prioritised on criticality, vulnerability and probability.
- Infrastructure, vehicles and operations need to be prioritised in order to most effectively use and distribute security resources, concentrating on potential high-risk assets.
- There is currently no substitute for the observance of abnormal or suspicious behaviour to the trained human eye.
- Available technologies need to be evaluated for their effectiveness as security devices, as well as their adaptability to other transportation objectives.
- Multi-faceted holistic layered approach, where each ‘check’ can compensate for failure or shortcomings in the preceding check, appears to offer an effective approach.

CONTENTS

1 BACKGROUND

This report represents the third deliverable of a research project funded jointly by Main Roads and Queensland Transport aimed at identifying the role which all levels of government can play in the process of implementing change in the freight logistics (FL) sector in Queensland. That role is primarily focused on the potential for economic efficiency gains and on the minimisation of any adverse environmental impacts resulting from freight transport.

Working Paper 1 provides a comprehensive review of national and international literature on the role for governments in the freight and logistics sector.

Working Paper 2 summarises the information gained from a series of interviews conducted amongst logistics professionals, from within Australian Fortune 50 companies. The object of the interviews was to gain a better understanding of the main issues that could impact the logistics industry in Australia, specifically in the future role of the creation of the virtual supply chain and ITS implementation. By highlighting and understanding potential future inhibitors, fears and concerns a greater understanding of the potential future needs for Government legislation and action was gained from the interviews.

The current report, Working Paper 3, examines one of the main issues highlighted in Working Paper 2, namely transport security. General security issues; concerns over the chain of responsibility regarding the implementation of security risk measures; and incident management followed a security breach, were seen by all the respondents as areas of concern. All respondents felt that there is an urgent need for further guidance and proactive action by governments.

This report examines those potential security threats which are of most concern and which may be acting as inhibitors towards the development of a ‘seamless’ integrated supply chain. Also discussed is relevant international evidence on tackling transport security risks.

The report creates a knowledge base from a significant body of global literature on the current state of security threat, and what governments and private organisations are implementing or proposing to implement to combat this threat.

The two main components of the report are:

- Review of literature. Open source papers, commissioned reports, and databases on the subject of terrorist attack minimisation, critical infrastructure protection and analysis, and the threats of digital and biological attack were reviewed. Areas of specific application to transport were analysed and summarised; and
- Application of 'threat' assessment. A proposed methodology for the assessment of 'critical prioritisation' of transport aspects based on the literature review and analysis of past events.

2 OVERVIEW

*'***Security** *and taking the necessary precautions is a* **cost** *of doing business because if there is an attack, if there is damage done, if there is a* **security breach** *which is serious enough, then that effects the bottom line,'[1]*

Since transportation began, transport vehicles, facilities and associated infrastructure have been subject to recurrent terrorist attacks, hijackings and sabotage [2, 3]. The 9/11 hijackers added a new dimension by using the hijacked airliners as deadly guided missiles.

Launching an informal summit and a new document titled 'Protecting Australia against Terrorism' outlining the Government's anti-terrorism initiatives, John Howard stated that the September 11 terrorist attacks cost the United States Government $US75 billion and that Australia 'is not immune from terrorists and businesses must be prepared', [4].

In its final report, the 9/11 Commission concluded that concern for such consequences is warranted and that little has been done to address the risks: 'While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation.',[5]

2.1 Transport Security

Transport security is the combination of preventive measures and human and material resources intended to protect transport vehicles, infrastructure, systems and workers against intentional unlawful acts [6]. The nature of transportation systems make them especially vulnerable, and hence attractive, to terrorists or other attackers [7].

The very nature of transportation and its vital function within both social and economic aspects, add up to the fact that in some way 'transport' or 'transport infrastructure' will always be a part of any attack. For example, to build a large explosive device, components

and materials have to be delivered by road/rail/ship or air. Weapons used in the attack have to be transported to the attack scene, armed attackers or suicide bombers have to travel to the place of attack. Similarly, any plan for incident management or recovery strategies may require the use of transport vehicles, transport infrastructure, and transport control. For example, the fast and decisive actions undertaken by the New York subway control centre, which stopped commuter and subway trains passing under the World Wide Trade Centre immediately after the attack, may have saved hundreds of lives [7] .

Hence, transportation is not only a potential and attractive target, but may also play a vital role in prevention and detention, in monitoring and mitigation, and additionally, in response and recovery.

Acts that threaten the security of transport include:

- International and domestic terrorism by:
    - Introducing something into a legitimate shipment and tampering with that legitimate shipment (e.g. tampering with consumables and contaminating them prior to delivery – e.g. bioterrorism);
    - Hijacking vehicles to replace cargo with explosive or toxic material and then using vehicle as a weapon;
    - Hijacking vehicles carrying hazardous materials to use as a weapon or using such vehicles as catalysts in an incident (e.g. placing a small explosive next to vehicles carrying highly explosive liquids or gases to increase the explosive impact);
    - Destroying or partially disabling transport infrastructure (e.g. bombing critical structures such as bridges, traffic control centres), thereby disabling the flow of transport and potentially slowing the incident response and recovery time;
    - Hacking into communication systems and either creating an incident (e.g. causing signal failure on critical railway corridors, airline control etc.) or disabling those systems and causing disruption;
    - Using legitimate vehicles as weapons of destruction (e.g. causing a derailment of carriages loaded with toxic and/or flammable material within the city corridor); and
    - Attacking vulnerabilities in the intersections and interactions between transportation modes and other domains such as energy and computer systems.
- Theft of goods in transport

- Natural or unpremeditated disasters which destroy or maim essential infrastructure or disable communication channels.

2.2 Definitions

Definition of terrorism: No one definition of terrorism has gained universal acceptance, however, for the purposes of this report, the following definitions have been adopted [8]:

- The term terrorism means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience;
- The term international terrorism means terrorism involving citizens or the territory of more than one country; and
- The term terrorist group means any group practicing, or that has significant subgroups that practice, international terrorism.

- Security is becoming a necessary and essential cost of doing business.
- Transportation is a potential and attractive target, that also plays a vital role in:
    - Prevention and detention
    - Monitoring and mitigation
    - Response and recovery.
- Growing reliance on virtual systems for control and monitoring opens up vulnerabilities in the communications and virtual transport networks.
- Threats to transport security can be in the form of:
    - Direct physical attack (bombing of infrastructure, hijacking, etc.)
    - Direct operation attack (viral attack on critical systems, tampering with communication channels, etc)
    - Tampering with legitimate cargo (introducing biotoxins, etc.)
    - Use of vehicles as weapons of destruction (9/11 attacks).
- Certain elements of the transport infrastructure (eg: the Sydney Harbour Bridge, and other landmarks, are cultural and Western symbolic icons, adding further appeal to terrorism targets.

3 SUPPLY CHAIN SECURITY - THE HIDDEN COSTS

3.1 Ignoring transport security: the economic cost

Any major security attack can have reaching implications and costs well beyond the initial 'damage' costs. The preliminary estimate for the cost to New York city economy and revenues was set at $US45 billion for 2001 and $60 billion for 2002 and 2003 [9, 10][1].

However, as many of the costs are qualitative and intangible, it is difficult to allocate specific costs to supply chains and the community at large for every transportation attack scenario. The total cost of an attack is dependent on the efficiency of response and incident management systems in place. For example, the avoidable problems in the interoperability of communication systems and bottlenecks and congestion in the communication channels has been quoted as the cause of loss of many lives [11].

Despite the difficulties in quantifying and forecasting potential effects, many efforts have been made to quantify the overall costs. Figure 1 shows an estimate made for an attack on a US maritime port. It highlights the potential delays and disruptions to the supply chain and the potential economic impact.

These estimates are generally conservative and typically only include direct costs. Not accounted for are the costs of cargo delays to parties at either end of the supply chain; costs of choosing alternative routes for transportation; and losses at the upstream or downstream end of the supply chain. Additionally, social costs such as trauma and subsequent loss of productivity and health problems are also not generally included in this type of cost estimation.

[1] Refer to Appendix A for a for a full cost summary of the 9/11 attacks.

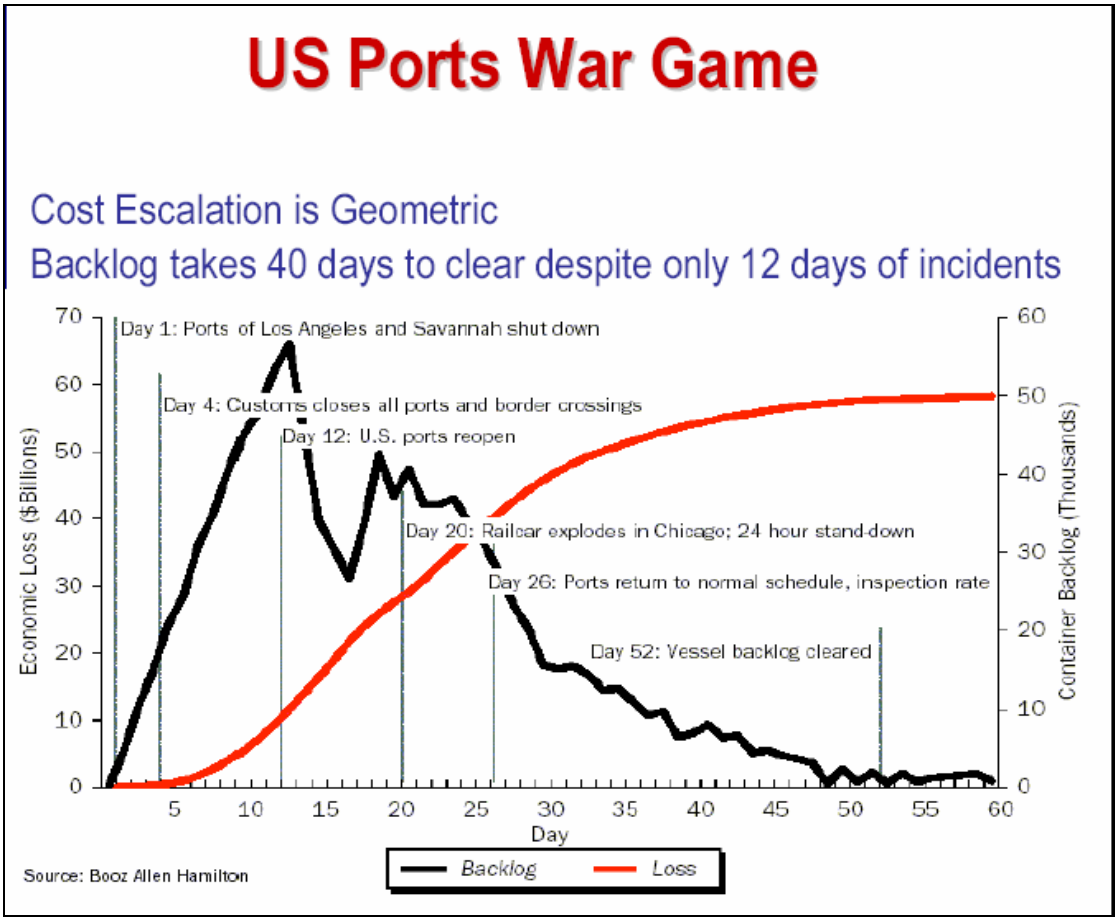

Figure 1 Example showing general estimate of potential costs[12]

3.2 Implementing transport security: the economic cost

Even a small attack can potentially cause massive disruption to supply chain operations and the community, both economically and socially. The detection and prevention of attacks can also potentially cause additional costs, disruptions and delays.

For example, the 24-hour rule which came into effect on the 2 December 2002 and was fully enforced as of 2 February 2003 states that carriers and importers are to submit a cargo declaration to the U.S. Customs 24 hours before cargo is loaded onto vessels with a port of call in the United States. The estimate for the cost of implementing this rule to the supply chain has been calculated at $US25/TEU (Twenty tonne equivalent unit) [13] . As a result, the subsequent annual cost to the Australian US export supply chain will rise significantly over time.

An example: Bioterrism.

In December 2003, in an effort to protect Americans from threats against bioterrorism: the U.S. Food and Drug Administration (FDA) required everyone who ships food to the U.S. to submit prior notices, part of a complex vetting procedure that can add thousands of dollars to the cost of doing business. A small family business; Johan De Greefs chocolate factory in Toronto reports that under the new rules 'he spends hours sorting out his chocolate turkeys from his truffle pumpkins, each of which requires a separate notice to U.S. authorities. Says De Greef: 'It used to cost me about C$25 each shipment for brokerage costs, but now it can be as high as C$400', [14].

Determining how much security is required is only part of the problem faced by a threat. The issue of who is to pay the additional cost of providing for security has also received some attention.

The very competitive nature of the transport business is likely to force the adoption of low cost solutions to provide security. Concentrated efforts may provide the minimum solutions in order to comply with international stipulated rules, above a minimal level, companies will not be able to make investments. Because security is a classic example of a public good, the expectation is that it will not be provided by firms beyond minimum levels required by law. Thus, it is up to government to answer questions concerning how much the nation is willing to pay for additional security, what organizations will be charged with ensuring it, and who should pay for it.

3.3 Technology

Many technologies, if used fully and efficiently, could potentially decrease or eliminate many of currently known security threats. However, the implementation of these technologies can be costly, and their use can potentially cause unwarranted delays and bottlenecks within the supply chain.

Additionally, as technologies, transport and supply chain operations and security threats are changing continuously, making long-term costly commitments to security technologies runs the high risk of early or prolonged obsolescence, unless the technologies are developed and deployed within a planned and efficient system context. For example, resources may be better utilised in the use of randomisation of many technology traps (random screening of cargo at intermodal, rail terminals and road checkpoints, random use of sniffer dogs) as opposed to one 'major consistent' check at one checkpoint.

Technology has a potential role in the detection and prediction of high-risk assets and activities via the use of sophisticated decision-making and assessment tools. Such intelligence techniques can be used as an aid to risk and vulnerability assessments to assist both Government and organisation decision makers to allocate security resources effectively in order to primarily target assets and activities which have been assessed as high-risk. Information gathered from currently used control and monitoring technologies, analysed via the use of artificial intelligence tools, may potentially offer an effective means to create a 'virtual' closed secure system.

- Any security attack can have reaching implications beyond 'damage' costs.
- Costs of implementing transport security may involve delays, productivity losses.
- Who will bear the costs 'user', 'polluter', or 'beneficiary'?
- Security is seen as a 'public good' - hence not an attractive 'investment' in the competitive market.
- Potential cost and magnitude of security task in the transportation sector means that it must be approached systematically and effectively.
- Intelligent decision making and assessment tools may potentially assist in the efficient allocation of security resources in targeting high-risk assets and activities.

4 SECURING THE SUPPLY CHAIN: THE PROBLEMS

4.1 Characteristics of transport systems

Partial or total physical destruction of some facilities and/or structures can totally or partially disable the network, causing massive disruptions to the supply chain function, potentially causing far-reaching and long-lasting economic and social effects [7].

Furthermore, vulnerabilities have been created by an increasing interdependence among complex networked systems, i.e. the growing integrated supply chain network. The issues of transport security have centred more on physical attacks than on to cyber attacks on real-time supervisory control and data acquisition systems that provide system status information and control the transport operation. Air traffic control, maritime and rail communications are currently more vulnerable to this type of attack. However, as security becomes further dependent on complex monitoring and control systems (track and trace, RFID, etc.), the system becomes more vulnerable and susceptible to being targeted in this manner.

Whether the threat be of a direct physical or 'virtual' one or indirect use of the transport function to disable or disrupt another system, transport systems are difficult to secure for the reasons discussed below.

4.2 Accessibility and susceptibility

Transport is primarily designed to be open and accessible for maximum private and public use. However, this accessibility means that access to many critical assets of the system, such as bridges, highways, etc. is completely unrestricted. To change this will take time and cost, methods of 'prioritising' the 'criticality and vulnerability' of certain aspects need to be devised and work concentrated preliminarily on integrating and heightening security in these areas.

Tightening of security has concentrated on access to airfields and airlines, with sophisticated systems being devised and implemented to screen passengers, luggage and freight, and monitor airline and airport workers. However, it would be both costly and time consuming to implement such a defensive and protective approach in land transportation. Even if all freight cargo workers were monitored and every commercial truck screened at regular checkpoints, it is still relatively easy to obtain a vehicle by legitimate means. For example, the most noted terrorist acts conducted in the United States involved legally leased trucks with legally obtained cargo (1993 World Trade Centre bombing in New York and the 1995 bombing of the Murrah Federal Building in Oklahoma City) [15].

4.3 Extent and Ubiquity

The Queensland network consists of a total of 178,290 km of roads with 38.5% of the total figure surfaced with bitumen or concrete. This is only approximately 22% of the total road network of Australia. At June 2004 there were almost 12.5 million motor vehicles (excluding motor cycles, tractors, plant and equipment, caravans and trailers) travelling throughout the Australian network, 18% of which are classified as light, rigid or articulated freight carrying vehicles. Australia's rail systems comprises of 41,286 km of broad, standard and narrow gauge track. This figure includes light rail systems, it also reflects private development, such as the 4,150 km narrow gauge system of the Queensland sugar industry. A total of 44,034 freight wagons travel this network (this excludes the 54,000 610mm sugar cane wagons). Queensland has 20 from the total of 97 appointed ports in Australia. Each one of these is a point of passenger and cargo entry into Australia or transfer where customs and quarantine activities are carried out. A total of 9,040 ships are registered in Australia, 2,884 in Queensland. Separate to these, at June 31, the Australian trading fleet consisted of 81 ships, capable of transporting a total of 1,764,298 gross tonnes/anum. Australia also has 261

licensed airports, and a total of 11,788 aircraft in the Australian Civil Aircraft Register, as at 31 December 2002 [16]. In addition, along this network are scattered fixed facilities such as bridges, operational control centres, maintenance bases, checkpoints, CCTV's and other monitoring devices.

Most of this infrastructure remains unguarded and unattended, most of the time. The extent and sometimes transience of these facilities makes them difficult to monitor and control. Currently, many technology measures do exist which would grant some control and monitoring capability of these facilities. However, several problems exist in their implementation:

- Cost;
- Time loss, inconvenience and disruption caused throughout the supply chain through extensive and thorough checking procedures;
- Lack of legislation as to requirements for monitoring and control;
- Lack of adequate guidance and legislation on security standards and integration of communication channels across the states; and
- Fears of ensuing privacy issues.

4.4 Emphasis on efficiency and competitiveness

Although infrastructure is mainly owned by the public sector, facilities that use that infrastructure are generally owned by the private sector. Low operating margins and competition make it difficult for freight companies to justify the internalisation (cost of implementation of security measures) of external (public sector) losses such as buildings, tunnels and bridges [15].

Despite National and State governments being responsible for the development and maintenance of most of the physical infrastructure, private companies and individuals function mainly as service providers and users of the network, and hence control most of the vehicles and containers that ply the networks.

Due to this diversity, and the transient nature of transport, many organisations, various authorities, carriers and members of the general public may find themselves 'involved' in the passage of one consignment or 'transport journey'. Hence, there is great difficulty in determining who is responsible for security. A single entity cannot be held responsible for defending each perceived vulnerability or 'loophole' along the supply chain.

Some external cost of security for essential infrastructure must be borne by the users that demand or rely on the integrity of that infrastructure.

Guidance should also be given as to what security measures are effective, in order that companies are not 'wasting' resources on implementing measures which are not effective or compatible with national standards or guidelines. Respondents from a recently conducted industry survey felt that this was an area where governments had a proactive role [18]. Some respondents expressed a feeling of being overwhelmed by the many technology options and a slight confusion as to 'how far their responsibilities lay'. Easy cost effective options, some of which are already under development in some areas are, include [15, 17]:

- Research, compile and disseminate lists of threat specific, low cost/no cost security measures and a guide for their application, to all carriers;
- Develop guidelines as to the chain of responsibility in various scenarios, develop a standard self-assessment tool for organisations to assess their risk and potential responsibility, so that they can evaluate and implement options and planning;
- Research current effectiveness of security-based measures and the 'duality' of these technologies (i.e. track and trace technology can be used as anti-theft and security measures as well as providing data and control for increasing the efficiency of the supply chain). Technologies that are dual purpose can be of benefit to both the freight company and society.

4.5 Chain of responsibility

This issue of the 'liability' or chain of responsibility was raised by all respondents during the industry surveys cited above [18]. Many respondents felt unsure as to how many preventative measures they were 'expected' to provide. All felt there was an urgent need for national standard Government guidelines on specific responsibilities for the prevention of threats, for monitoring and controlling, and for post incident management and recovery procedures.

The implementation of such technologies as RFID, track and trace, e-seals, etc, is in some cases being heralded as the panacea to the problem of security. However, these technologies also carry risks. Guidelines and legislations need to be set on the control and use of the information potentially obtained from these technologies, as well as the control of the integrity of the technology (i.e. monitoring access to unused seals). Issues of privacy (such as the debate over data mining and biometric technologies [19]) have inhibited many of these technologies progressing in the past, and there is reason to believe that these issues will

continue to be raised. Due to the sensitivity of these issues and potential abuse that the data collected from these technologies can be subject to, it is necessary for legislation to protect both the individual and the organisation from potential future litigation.

Assessing the 'chain of responsibility' is a complex issue, as the fundamental assumption of any complicated network survivability analysis and design is that no individual component of the system is immune from attacks, accidents, or design errors. The survivability of one component relies on the smooth operation of another[20]. This applies to the transport network as much as it does to a communication network.

Hence, in a system as complex as the transport network, and its even more complicated supply chain component, the only acceptable solution would be to provide a layered and holistic security system, with multiple check points and the co-operation of various parties. Each party would have specific deterrent, prevention and monitoring systems in place. Each providing backup to the other, hence perfect execution by each element in the system is not crucial, and failure by one layer has a chance to be picked-up by another.

The fact that sound security measures are necessary is indisputable, for it has been found that implementing security measures within the transport system deters terrorist operations, increased the likelihood of such operations being detected and stopped, minimises casualties and disruptions and reduces future trauma in the victims [2].

- Transport network is extensively diverse, necessarily accessible, ubiquitous and entwined in the economy and the community.
- Fully integrating security will take many decades, as new systems are developed and implemented, assets are gradually modified and replaced, standard guidelines and regulations are proposed and implemented.
- Diversity of users, owners and operators and the extent of the network create a system in which it is almost impossible to totally protect each potential target or perceived vulnerability.
- A potentially workable solution includes a layered and holistic approach.

5 THE INTEGRITY OF THE SUPPLY CHAIN: COMMON THREATS

5.1 Theft of goods in transit

This is an area which tends to receive little attention and yet many businesses suffer substantial losses. The fact that under-reporting is widespread, and that this kind of sabotage is both frequent and difficult to control, highlights the openness and accessibility of transportation systems and the difficulty of monitoring every movement. This fact is accentuated by the fear of freight-forwarders to report 'weak links' or 'security vulnerabilities' in fear of bad publicity and the loss of their supply of customers [21].

Additional reasons given for under-reporting are identified as [22]:

- Carriers frequently feared that shippers might shift business to another carrier due to security concerns;
- Carriers wanted to limit the ability of competitors to disclose their security record as part of efforts to gain market share;
- Carriers feared that insurance companies would use theft statistics to justify increased premiums for coverage; and
- Carriers were unable to determine the actual point of loss during a long or complex trip.

Yet the theft of so called 'hot products' which can disposed of in the black market, is known to be common [23].

In the US, annual cargo loss estimates range from US$3 billion to US$10 billion. Road transport is associated with approximately 87% of the total direct-cost value of the lost cargo, maritime approximately 8%, rail cargo 4%, and air cargo 1% [22, 26]. The fact that most of this theft is not being reported indicates the vulnerability, specifically of road transport to this form of security attack.

5.2 Threats to key infrastructure

Much work has been done by the Australian government and transport community to secure airports, and procedures are currently being devised and implemented to enhance the security in Australia's major ports. However, currently there appears to be little or no co-ordinated methodology or guidelines to secure other key infrastructure essential to the functioning of the state and national economies.

Given the extensive nature of land based transport, standard methodologies for determining its criticality and vulnerability and hence providing guidelines for its security, is imperative. Where opportunities arise, such as the design of new stations, protective physical features (such as blast resistance structures), as well as new technology (sensors that detect chemical and biological agents) can be added. However, as currently little of these measures are in place, the first step is to determine how to best filter the lower-risk infrastructure and transport users, in order to focus on security resources on anomalities and higher-risk traffic[7].

Road, rail and the various land transport participants are all currently implementing different measures in different ways and there exists no minimum security standards. There is currently little accurate information about internal shipments significantly reduces the potential for effective risk management and control. Intermodal movements provide vulnerable accessible points where a unit can be opened or tampered with and then passed onto to the next 'player' without the interference being noted. However, to avoid potential delays and disruptions whilst units/vehicles/carriages are being transferred there needs to be agreed procedures and technologies for the loading, sealing and locking of cargo.

The international nature of transport requires a national co-ordinated approach to security in the supply chain which is compatible with the procedures being implemented internationally.

5.3 Virtual attack

Little attention seems to have been paid to the vulnerability of the transport network to virtual attacks. Increasingly, the supply chain operation and its vital transport links are becoming dependent on complex virtual networks linked by potentially accessible communication channels.

A critical challenge is the ability to identify emerging virtual threats, and hence provide adequate measures for their prevention and post incident planning. This has been especially difficult when providing virtual security for several reasons:

- Currently investigations to this threat tend to be reactive and event-driven. While this has limited effectiveness for simple system intrusions, it will not be adequate for sophisticated attacks. Unless a more analysis-based process is employed, prevention will continue to lag behind the threat curve;
- The speed at which new technology is introduced creates a rapidly moving target for threat assessments. Each new technology requires high-level technical expertise to analyse. By the time vulnerabilities are identified technology has changed again;

- There appears to be a general lack of understanding of technology or the multi-dimensional aspects of information security. Many security professionals are biased toward a particular product such as intrusion detection systems or firewalls, this may limit the scope of proposed solutions; and
- Exaggeration of threats and capabilities by some security consultants and the press and the sympathetic portrayal of low-level intruders by others, have caused a counter-reaction dismissing potential threats.

Similarly to a physical attack, it is possible to accurately predict of exactly when, how, and by whom a potential threat will manifest itself is impossible. However, intelligence-driven analysis can detect specific enabling activity and other indicators that allow prediction of new threats. This information can be used in traditional risk assessments for better choice controls and provide justification for budget and resource decisions.

- Crime, especially in road transport is currently unreported, thereby increasing the difficultly in accurately assessing the vulnerabilities.
- Due to the extent of vulnerabilities and the potential cost of security, security efforts need to be dual-use, efficient and adaptable.
- Need to prioritise security criticality so that resources can be assigned effectively
- Need to mesh security measures with other objectives, such as curbing theft, tracking and monitoring cargo, asset management and assuring safe operations.
- Intelligence-driven analysis used to detect threats in the virtual network may be adaptable to use in the physical transport network. These methods can enhance the traditional risk assessment for better control and justification of budget and resource decisions.

6 SOMES INTERNATIONAL RESPONSES

This section summarises some of the ways in which transport security has been addressed in Europe and North America.[2]

6.1 Europe

Following the attacks of 9/11, the European Union immediately took measures to improve aviation and maritime security. Currently the Community is working with international organisations such as the International Civil Aviation Organisation (ICAO), International Maritime Organisation (IMO), International Labour Organisation (ILO), World Customs

[2] For more information on the subject the reader should refer to United States Department of State Report 'Patterns of Global Terrorism 2003' published April 2004 http://www.state.gov/s/ct/rls/pgtrpt/2003/

Organisation (WCO) and the United Nations Economic Commission for Europe (UN-ECE) [6].

The EC Regulation 2320/2002 ensures that common rules in the field of civil aviation security are implemented. Such rules include control of access of sensitive areas of airport and aircraft, training of airport workers, as well as the monitoring of passengers, luggage and freight..

In maritime, the Commission has issued a proposal that presents rules on ship security assessment, security plans, enhanced security equipment, such as alarms and Automatic Identification Systems, and the introduction of full time security guards on ships. Further work and another proposal is being pursued to address current port security assessments and consequent requirements. This includes a methodology for determining the required security levels bases on the concentration of threat. Procedures are being implemented to train staff on the control and implementation of security measures in ports.

In 2003, a proposal was put forward for a regulation to modify the Community Customs Code. This will enhance the current power of the role of customs in the security management of the EU's external borders. This new rule will establish rules for security standards of the transportation of freight across the EU borders, it will ensure that security measures for transport within the EU countries are compatible.

Although currently most of the work has been done in maritime and aviation, attention is being turned to land transportation and the EU is currently working with the UN-ECE (United Nations Economic Commission for Europe) on a security approach for the whole supply chain. This project is running concurrently with the project by the World Customs on the investigation of improvements to transport security and the adoption of the second Resolution on Security and Facilitation of the International Trade Supply Chain (June 2004). This resolution aims to provide an international framework for security and facilitation and is the first step in the development and definitions of standards on integrated supply chain security and facilitation. Guidelines will be developed to assist developing countries to confirm to the standards that will be set [27].

The European Union recognises that it is essential that all current proposals and new transport security developments are compatible with developing international requirements and hence is ensuring that a common approach to transport security is undertaken[6].

6.2 United States of America (US)

Since the 9/11 attacks, the US has been heavily involved in the 'War against terror' [3] . Various reports and guidelines have been published, these include:

- *The National Strategy for Homeland Security*
- *The National Strategy for Combating Terrorism*
- *The National Strategy to Combat Weapons of Mass Destruction*
- *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*
- *The National Strategy to Secure Cyberspace*

The involvement and the response of the USA to the threat of terrorism appears to have been the greatest of all the Western nations. However the Bush administration has come under criticism for its lack of security implementation within the land transportation sector. It is felt that there is still insufficient control on trucks carrying hazardous materials, and that proposals for the implementation of security measures to confirm the identification and authenticity of drivers within the industry have not been implemented. Additionally shipments by rail of hazardous and radioactive material on corridors close to US major cities are continuing, despite federal government promises to tackle these issues.

6.3 Canada

Rail: Canada also has implemented many security measures, with a complete review of its rail sector security. Transport Canada has increased the security of passenger rail transportation at critical locations and facilities through the implementation of detailed security plans.

Transport Canada is also working with the Railway Association of Canada on the further development and testing of security and emergency plans, the exchange of information and incident reporting [28].

Road: Actions has been taken to enhance security at strategic locations such as bridges and tunnels, and to increase awareness of security in the transportation of dangerous goods. From October 2001, Transport Canada's dangerous goods inspectors began visiting all operators who hold Emergency Response Plans (ERAP) to provide security awareness briefings. New rules demand that the validity of driver's licenses be verified whenever an inspection of a truck transporting dangerous goods is undertaken. Every effort is being undertaken with other

[3] See Appendix B for a surmised listing of US combating terrorist actives in 2003

departments and agencies involved in the inspection and transportation of dangerous goods to coordinate all efforts in the security of transportation of dangerous goods.

Maritime: IN April 2004, Deputy Prime Minister Anne McLellan announced the National Security Policy, which set out a six-point, $308 million program to support marine security[4].

6.4 Australia and New Zealand

Following the 9/11 attacks, the Australian Government committed $800 million over five years to strengthen Australia's domestic security, supplemented by a further $60 million after the bombings in Bali. In the interests of protecting Australia's vital assets, a Critical Infrastructure Advisory Council was set up, involving the Commonwealth, State and Territory governments, State and Territory police and, importantly, the owners and operators of critical infrastructure.

In 2001, the Australian Federal Government enacted a Cyber crime Act, to give federal law enforcement agencies the authority to investigate and prosecute groups who use computer networks to plan and launch cyber-attacks. The police have also been given new electronic investigation powers. Law enforcement officers can now compel someone with knowledge of a computer system to provide the key to encrypted data, and also gives police clear authority to search for evidence on computer networks extending across different locations.

Aviation: An Aviation Transport Security Bill introduced in to Parliament in 2003 provides a foundation for an overhaul of the aviation security policy framework. The legislation addresses the fundamental elements of the aviation security regulatory arrangements and clarifies roles and responsibilities for the aviation industry, the Government and the travelling public. The Australian government has announced the requirement to tighten access to airside areas of airports and the requirement to carry aviation security identification cards will be extended to more airports, and there will be a national reissue of the cards in 2003-04. By December 31st 2004, one hundred percent checked baggage screening on all international flights and the introduction of checked bag screening at all major domestic terminals will be in place.

Maritime: Significant developments in preventative security have also recently taken place in the maritime sector. In recognition of the importance of the maritime sector to Australia's national interests, the Australian Federal Government supported the December 2002

[4] Refer to http://www.tc.gc.ca/mediaroom/releases/nat/2004/04-gc005ae.htm for additional information.

International Maritime Organization (IMO) action to strengthen international preventive maritime security measures. These measures include the new IMO Ship and Port Facility Security Code.

A Maritime Transport Security Bill was implemented in 2003. The Australia Department of Transport and Regional Services is currently working with a range of agencies, to develop a range of measures aimed at improving supply chain security within Australia, in response to U.S. requirements for Australian containerized exports to the U.S., and the Secure Trade in the APEC Region (STAR) initiative.

The Queensland government has been following these initiatives in addressing surface transport security. In particular, governments are working through priorities identified in the National Transport Security Strategy. For example, the newly introduction of anti-terror fertiliser restrictions, governing the use and transportation of ammonium nitrate [29].

7 SECURITY NEEDS ASSESSMENT

7.1 Vulnerability, Probability and Criticality (VPC)

Critical infrastructure includes both physical and cyber-based components, which are used in attaining transportation functions to serve national, regional and local objectives [30]. Hence the vulnerabilities need primarily to be categorised into three main infrastructure groups;

1. The physical infrastructure and facilities themselves;
2. The vehicles that operate on the system; and
3. The information or 'virtual' system which monitors and managers the users and cargo flowing through the network.

Infrastructure needs to be prioritised on the basis of vulnerability, probability and criticality (VPC), as shown in Figure 2:

- Hierarchy of impact (consequence)
- Current state of asset (vulnerability)
- Hierarchy of opportunity (probability)
- Iconic status (relevance or proximity to national or 'Western' icons[5])
- Recovery aspect (capacity to recover and reconstitute normal operation)

[5] Analysis of events in 2003 showed Western 'icons' such as MacDonalds, Shell or Caltex terminals, are continuously targeted, hence infrastructure or parts of infrastructure located in proximity to these icons is potentially a more attractive target.

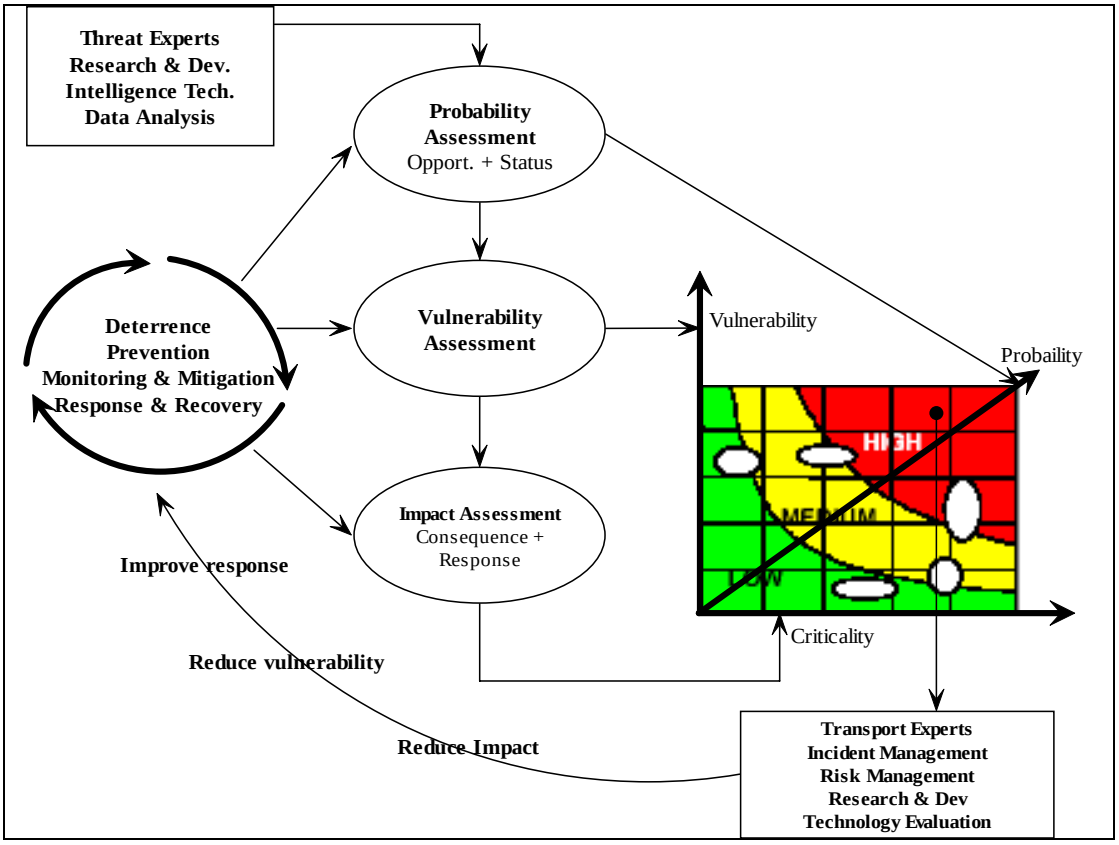

Figure 2 Assessing 'VPC' vulnerability, probability and criticality (adapted from SIAC[32])

Assets need to be identified and then their priority evaluated in regards to their 'VPC' score. Priority assets are then assessed to review whether simple low-cost security preventative and deterrence methods can be implemented (such as better lighting, emergency evacuation routes, content filtering software, etc.). It is at that this point that consideration must be given to the crucial and important security function of staff such as station attendants, ticket collectors, bus and train drivers, cleaners and maintenance personnel. Advancements in technology may render surveillance systems that are far superior, but currently there is no substitute for the observance of abnormal or suspicious behaviour than the trained human eye. It is essential that such staff receive training to recognise, react and respond appropriately to such incidents, as they are often the first on the scene. Cleaning and maintenance staff spend their working day looking in places where weapons may be hidden (i.e. under and behind fixed furnishings etc.). Additionally, the general public are an important resource, whether it is to look for and report unattended articles or report suspicious behaviour. Use of other specific but low-cost options may involve random use of chemical/explosive-sniffing dogs at intermodal terminals, railway yards or truck stops.

If deterrence and prevention (guards, fences, locks, firewalls) are unsuccessful or not available under low cost options, implementing systems for monitoring and mitigation and devising effective post-event response plans is the next line of response. Communication channels, necessary equipment and strategies must be planned in advance as part of incident management plans. To recover quickly and reconstitute the normal traffic operation is crucial in limiting the economic costs of an attack. Hence, possible alternative routes for major traffic flows needs to be assessed and checked whether it is possible to integrate with current systems. Part of the plan should include traffic control and alternative routes that can work effectively, causing minimum disruption and chaos, and re-directing all traffic from contaminated areas quickly and effectively.

Once all of these factors have been evaluated the asset can be reassessed for its priority. If it still falls in the high priority, then higher cost solutions need to be explored. Currently, many of the more sophisticated technologies being proposed for security purposes have only limited potential for application. Many technologies that seem promising in isolation may not work well within the transport system environment [7].

Available technologies need to be evaluated for their effectiveness as a security devices as well adaptability to other transportation objectives. Carriers may be able to justify the cost of implementing systems of security such as e-seals, blast-resistant containers, etc. if they also enhance the productivity of the logistics chain and secure their cargo from theft and loss [32]. Similarly, when evaluating the implementation of e-business, logistics and related technology, the benefits gained in enhancing the security aspect should be included as a benefit in the evaluation. A system of subsidies may have to be put in place to encourage small to medium companies to include national security objectives in the transportation planning process. Such incentives may need to be directed at the manufacturing level - designing and building vehicles, carriages and containers; as well as designing and implementing operating and communication systems.

7.2 Further research

Prioritising assets for vulnerability, criticality and probability provides a simple but powerful framework to assess security needs. How best to assess and evaluate these factors in order to focus security resources on high-risk aspects requires further research. Much data from previous attacks, threats and the consequences exist, and this data would be useful in identifying significant markers and indicators. However, data on crime within the transport sector, specifically theft and loss, goes mainly unreported, and this data would also be critical

to highlight current vulnerabilities. With the implementation of such technologies as RFID, more of this data will become available. Currently, there is a wealth of transportation data which is being collected by various sources, and not being collated and analysed, either to drive efficiencies within the supply chain or to analyse security prevention and detection.

Available historical data has the potential to be analysed using advanced artificial intelligence tools to produce some useful results for detection and control purposes.

The concept of a holistic and layered security system, integrated with transport operations, where multiple security features are connected and provide back-up for each other, has many advantages. Each element may be crucial, but failure by one does not mean failure of the whole system. An attacker will find it more difficult to overcome multiple, random and entwining checks. Hence, such a system would appear to be more workable in the transport environment, where it is impossible to cover every vulnerability. Queensland Rail (QR) adopted such a multi-faceted approach in managing the security of its Citytrain network. This approach and how it has been performing could be further researched and developed in order to extend the concept to cargo and other nodes of transport [33].

- Infrastructure needs to be prioritised on criticality, vulnerability and probability.
- Infrastructure, vehicles and operations need to be prioritised in order to most effectively use and distribute security resources, concentrating on potential high-risk assets.
- There is currently no substitute for the observance of abnormal or suspicious behaviour to the trained human eye.
- Available technologies need to be evaluated for their effectiveness as security devices, as well as their adaptability to other transportation objectives.
- Multi-faceted holistic layered approach, where each ‘check’ can compensate for failure or shortcomings in the preceding check, appears to offer an effective approach.

8 CONCLUSIONS

The broad subject of vulnerabilities, probable responses and ensuing consequences needs to be evaluated in order to build a broad database of possible scenarios form which to assess the vulnerability and criticality of current transport operations and infrastructure. This needs to

be done in order to help the decision maker in allocating security resources and imposing standards, guidelines and regulations.

Further information and analysis is required to understand the exact nature of how the transportation and supply chain operation will be affected in various threat scenarios and to achieve a broader understanding of terrorist threats.

Prevention and detection, monitoring and mitigation, response and recovery systems need to be put in place, in order to reduce the likelihood of further attacks occurring in the future. An assessment of low-cost, easily implemented, effective solutions needs to be made with guidelines and standards for their implementation. Evaluation on the more advanced and sophisticated security technology needs to be carried out, with technologies being evaluated for their additional transportation operation enhancing functions, as well as their security benefits. Guidelines for new infrastructure, vehicles, communication systems and traffic monitoring and control functions need to be put into place to ensure consideration of all the possible security enhancements that can be added at little or no cost at the design and/or implementation stage.

REFERENCES

1. Howard, J., *Howard hosts anti-terrorism summit for business.* ABC Online, 2004.
2. Jenkins, B.M., *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview,*, in *Report No. MTI-01-14,*. 2001, Norman Y. Mineta Institute for Surface Transportation Policy Studies, San Jose State University,: San Jose, Calif.
3. National Research Council, *Improving Surface Transportation Security: A Research and Development Strategy,*. 1999, National Materials Advisory Board, Transportation Research Board, and Computer Science and Telecommunications Board, National Academy Press, Washington, D.C.: National Academy Press, Washington, D.C.
4. ABC Online, *Howard hosts anti-terrorism summit for business.* 2004.
5. The 9/11 Commission Report, *Final Report of the National on Terrorist Attacks Upon the United States*. 2004, NY: WW Norton & Company.: New York,. p. 391.
6. European Commission, *Freight Transport Security*. 2003, EC : Directorate-General for energy and transport: Brussels.
7. National Research Council, *Making the nation safer; The role of science and technology in countering terrorism.* 2003, The national Academies Press: Washinton DC.
8. State, U.S.D.o., *Patterns of global terrorism 2003.* 2004.
9. Hevesi, A.G., *The impact of the September 11 WTC attack on NYC's economy and city revenues (preliminary)*. 2001, The City of NY Office of the Comptroller: New York.

10. Editor summary, *9/11 by the Numbers*, in *New York metro.com*. 2004: New York.
11. Lund, D.A., *Learning to talk: The lessons of non-interoperability in public safety communication systems*, in *The ATLAS Project: Advanced technology in Law and Society*. 2002, University of New Hampshire.
12. Meyrick, S. and A. King, *Key issues in freight transport security*. 2004, Meyrick and associates.
13. Moller, A., *U.S Customs 24-hour advance vessel manifest rule*. 2003, Maersk Logistics.
14. Handelman, S., *How the war on terrorism hurts Canadian exports of wine and chocolate*, in *Time Canada*. 2004. p. 30.
15. Transportation Research Board, *Security Measures in the Commercial Trucking and Bus Industries*. 2003, Sponsored by Federal Motor Carrier Safety Administration: Washington DC.
16. Statistics, A.B. S., *Year Book Australia: Transport Infrastructure*. 2004.
17. American Trucking Associations, *"The American Trucking Industry's Anti-terrorism Action Plan,"*. 2002: Alexandria, VA.
18. Transport@QUT, *Role of Governments in Freight Logistics: Working Paper 2: Industry Interviews*, 2004, QUT, Brisbane.
19. Computer Science and Telecommunication Board (CSTB), *IDs - Not That Easy: Questions About Nationwide Identity Systems*. 2002, National Academy Press: Washington, D.C.
20. Farrell, A., L. Lave, and G. Morgan, *Bolstering the Security of the Electric Power System.* 2002.
21. Mayhew, C., *No.214 The detection and prevention of cargo theft*. 2001, Australian Institute of Criminology.
22. National Science and Technology Council, *Intermodal Cargo Transportation: Industry Best Security Practices*. 1999.
23. Clarke, R., *Hot products: Understanding, Anticipating and reducing demand for stolen goods.* Police Research Series, 1999. **112**.
24. Salkin, S., *Safe and Secure.* Warehouse Management, 1999. **10**.
25. Merklin, J.E., *Thieves at work. Employee fraud can take a toll on you company's bottom line.* Warehouse Management, 2004.
26. Salzano, J. and S. Hartman, *Cargo Crime.* Transnational Organised Crime, 1997. **3**(1): p. 39-49.
27. Organisation, W.C., *WCO Council adopts Second Resolution on Security and Facilitation*, in *Press Release by World Customs Organisation*. 2004.
28. Canada, T., *Enhancing transport security*. 2004, Transport Canada: Major Issues: Security.
29. News, A.P., *Queensland introduces ant-terror fertiliser restrictions.* Australia/New Zealand Reference Centre, 2004.
30. Haimes, Y.Y., et al., *Risk Assessment and Management of Engineering Systems*. 2004, Viginia Department of Transportation: Charlottesville, Virginia.
31. Science applications International Corporation, *A Guide to Highway vulnerability assesssment for critical asset identification and protection*, in *National Cooperative Highway and Transportation Officials Security Task Force*. 2002, The American Association of State Highway and Transportation Officials Security Task Force.

32. Badolato, E., *"Cargo Security: High-Tech Protection, High-Tech Threats,"*. TR News,, 2000. **211**(November-December): p. pp. 14-17.
33. McAlpine, R.J. *Queensland Rail's Citytrain Security System: An integrated approach*. in *The Second Australasian Women & Policing Conference*. 1999. Brisbane.

APPENDIX A: 9/11 ATTACKS: SOME STATISTICS

- Total number killed in attacks (official figure as of 9/5/02): **2,819**
- Number of firefighters and paramedics killed: **343**
- Number of NYPD officers: **23**
- Number of Port Authority police officers: **37**
- Number of WTC companies that lost people: **60**
- Number of employees who died in Tower One: **1,402**
- Number of employees who died in Tower Two: **614**
- Number of employees lost at Cantor Fitzgerald: **658**
- Number of U.S. troops killed in Operation Enduring Freedom: **22**
- Number of nations whose citizens were killed in attacks: **115**
- Ratio of men to women who died: **3:1**
- Age of the greatest number who died: **between 35 and 39**
- Bodies found "intact": **289**
- Body parts found: **19,858**
- Number of families who got no remains: **1,717**
- Estimated units of blood donated to the New York Blood Center: **36,000**
- Total units of donated blood actually used: **258**
- Number of people who lost a spouse or partner in the attacks: **1,609**
- Estimated number of children who lost a parent: **3,051**
- Percentage of Americans who knew someone hurt or killed in the attacks: **20**
- FDNY retirements, January–July 2001: **274**
- FDNY retirements, January–July 2002: **661**
- Number of firefighters on leave for respiratory problems by January 2002: **300**
- Number of funerals attended by Rudy Giuliani in 2001: **200**
- Number of FDNY vehicles destroyed: **98**
- Tons of debris removed from site: **1,506,124**
- Days fires continued to burn after the attack: **99**
- Jobs lost in New York owing to the attacks: **146,100**
- Days the New York Stock Exchange was closed: **6**
- Point drop in the Dow Jones industrial average when the NYSE reopened: **684.81**
- Days after 9/11 that the U.S. began bombing Afghanistan: **26**
- Total number of hate crimes reported to the Council on American-Islamic Relations nationwide since 9/11: **1,714**
- Economic loss to New York in month following the attacks: **$105 billion**
- Estimated cost of cleanup: **$600 million**
- Total FEMA money spent on the emergency: **$970 million**
- Estimated amount donated to 9/11 charities: **$1.4 billion**
- Estimated amount of insurance paid worldwide related to 9/11: **$40.2 billion**
- Estimated amount of money needed to overhaul lower-Manhattan subways: **$7.5 billion**
- Amount of money recently granted by U.S. government to overhaul lower-Manhattan subways: **$4.55 billion**
- Estimated amount of money raised for funds dedicated to NYPD and FDNY families: **$500 million**
- Percentage of total charity money raised going to FDNY and NYPD families: **25**
- Average benefit already received by each FDNY and NYPD widow: **$1 million**
- Percentage increase in law-school applications from 2001 to 2002: **17.9**
- Percentage increase in Peace Corps applications from 2001 to 2002: **40**
- Percentage increase in CIA applications from 2001 to 2002: **50**
- Number of songs Clear Channel Radio considered "inappropriate" to play after 9/11: **150**
- Number of mentions of 9/11 at the Oscars: **26**
- Apartments in lower Manhattan eligible for asbestos cleanup: **30,000**
- Number of apartments whose residents have requested cleanup and testing: **4,110**
- Number of Americans who changed their 2001 holiday-travel plans from plane to train or car: **1.4 million**
- Estimated number of New Yorkers suffering from post-traumatic-stress disorder as a result of 9/11: 422,000

APPENDIX B: TRANSPORT SECURITY IMPLEMENTATION IN THE US (2003)

Funding Summary – Border and Transportation Security

Border and Transportation Security
(budget authority in millions of dollars)

	2002 Enacted	2002 Supplemental	2003 Enacted	2003 Supplemental	2004 Request
Department of Agriculture	61.2	31.5	176.6	---	108.8
Department of Homeland Security	8,005.0	3,765.0	13,545.0	1,778.0	14,053.4
Department of Justice	8.1	6.0	25.4	---	31.1
Department of State	426.0	25.0	591.8	---	779.0
Department of Transportation	537.3	703.0	241.3	---	67.4
Department of the Treasury	8.0	---	---	---	---
Total, Border and Transportation Security	**9,045.7**	**4,530.5**	**14,580.1**	**1,778.0**	**15,039.7**

Major Agency Roles and Missions Summary – Border and Transportation Security

Department/ Agency	Agency Roles and Missions
Agriculture	*Animal and Plant Health Inspection Service* • Perform agricultural quarantine activities and risk analysis at ports of entry

Homeland Security	*Bureau of Customs and Border Protection* • Conduct inspections at ports of entry to detect and prevent illegal people and goods, including agricultural products, from entering the U.S. • Establish information systems to control arrival or departure of people and goods into the U.S. and target high-risk people and goods for further inspection and investigation • Detect, track, intercept and apprehend border threats between ports of entry • Work overseas to strengthen U.S. defenses against illegal smuggling and immigration *Bureau of Immigration and Customs Enforcement* • Investigate and enforce laws against the unlawful presence of people and goods into the U.S. *Bureau of Citizenship and Immigration Services* • Administer the visa petition and immigration process to ensure against issuance of immigration benefits to terrorists or persons who violate immigration laws *Transportation Security Administration* • Perform aviation security activities, including passenger and baggage screening, air marshals, and air cargo security • Develop systems to improve passenger screening and detect dangerous materials • Coordinate development of security measures for non-aviation modes, such as land transportation *United States Coast Guard* • Lead port security activities • Disrupt and interdict illegal maritime activities • Patrol ports and waterways • Screen high-interest vessels • Enforce security zones around key vessels and infrastructure • Place armed sea marshals on high-interest vessels • Conduct port security assessments and develop security plans • Review security assessments and plans of vessels and facilities

State	*Administration of Foreign Affairs* • Administer visa program to ensure against travel into the U.S. by terrorists, persons whose presence may be inimical to U.S. national security interests, or persons who violate immigration laws